**AFFIDAVIT OF SPECIAL AGENT ANDREA SCIOLINO IN SUPPORT OF A CRIMINAL COMPLAINT AND AN APPLICATION FOR A SEARCH WARRANT**

I, Andrea Sciolino, state:

***INTRODUCTION AND AGENT BACKGROUND***

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") and have been so employed since July 2017. I am assigned to the Economic Crimes Squad in the FBI's Boston, Massachusetts Field Office. My duties include investigating money laundering, wire fraud, and internet fraud. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, and electronically-stored information. I have received extensive training and experience in assessing various financial instruments and transactions and currently hold an active Certified Public Accounting license in the state of Florida. I hold a master's degree in Accounting with a concentration in Taxation.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I submit this affidavit in support of a criminal complaint against Yannick A. Minang a/k/a "Africa" (the "Target Subject" or "Minang"), as a basis for probable cause that Minang conspired with others known and unknown to the government to transport, transmit, and transfer, and attempt to transport, transmit, and transfer a monetary instrument and funds from a place in the United States to and through a place outside the United States, knowing that the monetary instrument and funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission, and transfer was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, in

violation of Title 18, United States Code, Sections 1956(a)(2)(B)(i) and 1956(h) (the "Target Offense").

4. I further submit this affidavit in support of an application for a warrant pursuant to Federal Rule of Criminal Procedure 41 to search the residence of the Target Subject at 319 Lincoln Street, Apartment 231, Hingham, Massachusetts, as described more specifically in Attachment A, for the purpose of seizing evidence, fruits, and instrumentalities of the Target Offense, as well as violations of Title 18, United States Code, Sections 1343 (Wire Fraud), 1349 (Wire Fraud Conspiracy), Section 1956 (Money Laundering), Section 1956(h) (Money Laundering Conspiracy), and 1512 (Witness Tampering) (collectively, the "Target Offenses"), as more particularly described in Attachment B.

5. As further discussed below, there is probable cause to believe that the Target Subject has committed the Target Offenses. There is further probable cause to believe he possesses computers and other evidence and instrumentalities of the Target Offenses at his residence, as described in Attachment B.

6. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the complaint and the requested warrant and does not set forth all of my knowledge about this matter.

## ***PROBABLE CAUSE***

### I. The Target Subject

7. The Target Subject, Yannick Minang, was identified in connection with an ongoing investigation into a type of fraud referred to as "business email compromise," ("BEC") which is a sophisticated scam often targeting businesses involved in wire transfer payments. The fraud is carried out by compromising and/or "spoofing" legitimate business email accounts

through social engineering or computer intrusion techniques (including obtaining credentials through "phishing") to cause employees of the target company (or other individuals involved in legitimate business transactions) to conduct unauthorized transfers of funds, most often to accounts controlled by the scammers. This type of fraud can take many forms and can violate several federal criminal statutes including, among others, the Target Offense.

8. Minang is due to be sentenced next month for his role in a similar, though different, BEC scheme in 2017. *See United States v. Minang*, 17-cr-10376-FDS. In that case, on January 23, 2019, Minang pled guilty to a five-count Indictment, pleading guilty to International Money Laundering, in violation of 18 U.S.C. § 1956(a)(2)(B)(i) (Count 1), Structuring to Avoid Reporting Requirements, in violation of 31 U.S.C. § 5324(a)(3) (Count 2), Unlawful Money Transaction, in violation of 18 U.S.C. § 1957(a) (Count 3), Concealment and Avoiding Reporting Requirements Money Laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and (ii) (Count 4), and Making a Material False Statement, in violation of 18 U.S.C. § 1001(a)(2) (Count 5) (the "2017 Conduct").

9. In connection with that case, on September 29, 2017, the FBI executed a search warrant at Minang's residence at the time, 800 West Street, Unit 1417, Braintree, Massachusetts. During the execution of the warrant, agents seized a computer and four mobile phones. In addition, agents seized numerous bank records kept by Minang at his residence.

10. I have learned from information provided by the United States Probation Office ("Probation Office") that Minang recently moved into a new residence at 319 Lincoln Street, Apartment 231, Hingham, Massachusetts, and is living there with at least two individuals who have been associated with other BEC schemes. I believe there is probable cause that Minang's current residence contains evidence, fruits, and instrumentalities of the Target Offenses,

including one or more mobile telephones that Minang has used in furtherance of the Target Offenses, as further described below.

11. As set forth below, there is probable cause that Minang has been engaged in criminal conduct very similar to the 2017 Conduct. I therefore believe that there is probable cause that his current residence contains evidence, fruits, and instrumentalities of criminal conduct very similar to that found in his residence in 2017.

II. The Target Subject Recruits Cooperating Witness-1

12. As further described below, since the 2017 Conduct, Minang has recruited and directed one or more individuals to open bank accounts in the name of sham companies in the District of Massachusetts, in connection with an apparent BEC scheme.

13. One such individual is "Cooperating Witness-1" ("CW-1"), who stated that they met Minang in 2018 while working as part of the wait staff in a Boston nightclub. CW-1 told FBI agents that Minang and his friends would come to the nightclub and spend thousands of dollars a night on so-called "bottle service."

14. At some point during the fall of 2018, Minang told CW-1 that he had a way for CW-1 to make additional money, which involved CW-1 opening one or more bank accounts for the purpose of receiving and then transferring and withdrawing funds. CW-1's understanding was that CW-1 would receive approximately 10 percent of the funds moved through the accounts as CW-1's share of the proceeds. Minang told CW-1 that by doing it this way, he and his associates would be able to transfer funds more efficiently, saving on fees and other expenses.

15. On May 20, 2019, FBI agents executed a search warrant for CW-1's person and mobile telephone. *See* 19-mj-1085-DLC. A search of CW-1's mobile telephone revealed that

CW-1 used the app WhatsApp to communicate with Minang and others in furtherance of the scheme.[1]

16. FBI agents found WhatsApp text messages on CW-1's phone between CW-1 and a person known to CW-1 as "Africa," who used the WhatsApp account associated with the telephone number [redacted]. During a subsequent interview of CW-1 by the FBI, CW-1 showed agents a picture of the person CW-1 knows as "Africa." I have been able to confirm that that individual is Minang.

17. In addition to the contact entry for the [redacted] number, there were three additional contact entries for "Africa" found on CW-1's phone: one contact name listed as "Africa," at telephone number [redacted] the second contact name listed as "Africa New," at telephone number [redacted]; and the third contact name listed as "Africa Room Décor," at telephone number [redacted]. Minang used this third phone number ("Africa Room Décor") at the time of the 2017 Conduct, and he has provided the same telephone number to the Probation Office.

18. In addition, "Individual-1" and "Individual-2" told the FBI that they were recruited by CW-1 to open bank accounts in the District of Massachusetts in furtherance of one or more BEC schemes.

19. CW-1 told Individual-1 about an individual involved in those schemes called "Africa." Individual-1 told the FBI about a time that CW-1 drove Individual-1 to the bank to

[1] WhatsApp provides internet-based calling and multimedia messaging services via mobile device software applications that function using cellular (e.g., Verizon, Sprint, AT&T, T-Mobile) or wireless (e.g., a Wi-Fi access point) data connections. WhatsApp communications are routed through the internet using a device's cellular or wireless data connection. By using a mobile device's data connection, WhatsApp offers an alternative to traditional calling, cellular short message service (SMS) and multimedia service (MMS), and allows a user to avoid calling, SMS, and MMS charges that cellular providers may charge for those services.

withdraw funds. After this transaction, Individual-1 was in CW-1's car with CW-1 and a man that Individual-1 assumed was "Africa." During this encounter, Individual-1 had an argument with CW-1 over the amount that Individual-1 would be paid for the transaction. Individual-1 later recognized a photograph of Minang as the man who was with them in the car.

20. Individual-2 advised the FBI that they had met "Africa" in connection with the schemes, and recognized a photograph of Minang as that individual.

21. At CW-1's request, Individual-1 opened two bank accounts in the name of sham companies: one at Bank of America in the name of "Sadia BRF SA," and the other at Santander Bank in the name of "Cvale SA." Bank records for those two accounts show incoming wire transfers to the accounts from , , , and ; and outgoing wire transfers from the accounts to and .

III. The Target Subject Directs CW-1 To Open A Santander Account

22. On or about November 23, 2018, at Minang's direction, CW-1 obtained a business certificate from the Town of Braintree, Massachusetts, for "BRF GLOBAL SA."[2] The certificate stated that the location of the business was 800 West St. 3402, and listed CW-1 as the sole owner of the purported business.

23. The following day, on November 24, 2018, at Minang's direction, CW-1 opened a "Business Checking" bank account at Santander Bank branch 0704 in Quincy, Massachusetts, in the name of "BRF Global SA," account number ending in 0965 (the "Sant-0965 Account").

[2] BRF Global SA, is, in fact, a Brazil-based multinational food giant, with American Depository Receipts ("ADR") trading on the New York Stock Exchange under the ticker symbol ("BRFS").

24. CW-1 told the bank that the business was a sole proprietorship, and the nature of the business was "interior design services." CW-1 provided the bank with a copy of the business certificate CW-1 had obtained from the Town of Braintree for BRF Global SA the day before. CW-1 deposited $200 to open the Sant-0965 Account, with funds that were provided by Minang.

25. According to bank records, as of December 24, 2018, the balance in the Sant-0965 Account was -$60.95.

26. On or about December 26, 2018, $9,845 was wired into the Sant-0965 Account from the account of [redacted] at The National Commercial Bank, Jeddah, Saudi Arabia, for "Buying Goods."

27. The following day, December 27, 2018, at Minang's direction, CW-1 withdrew the following funds from the Sant-0965 Account: (i) $6,000 at a Santander branch in Dorchester – Columbia Park; (ii) $3,000 at a Santander branch in Boston – Harrison Beach; and (iii) $380 at a Santander branch in Braintree. CW-1 gave this cash to Minang, who returned approximately $2,000 to CW-1, for CW-1 to keep.

28. On or about January 24, 2019, $15,000 was wired into the Sant-0965 Account from the account of [redacted] at First Caribbean International Bank, St. John's, Antigua.

29. On or about January 28, 2019, $15,450 was wired into the Sant-0965 Account from the account of [redacted] at First Caribbean International Bank, St. John's, Antigua.

30. That same day, on January 28, 2019, at Minang's direction, CW-1 withdrew the following funds from the Sant-0965 Account: (i) $6,000 at a Santander branch in Randolph –

North Main Street; (ii) $7,000 at a Santander branch in Holbrook; and (iii) $1,100 at a Santander branch in Braintree.

31. On January 30, 2019, at Minang's direction, CW-1 withdrew the following funds from the Sant-0965 Account: (i) $8,000 at a Santander branch in Randolph – North Main Street; (ii) $6,000 at a Santander branch in Quincy; and (iii) $1,460 at a Santander branch in Braintree. Following these withdrawals, there was $26.78 left in the Sant-0964 Account.

32. On or about February 5, 2019, $19,400 was wired into the Sant-0965 Account from the account of [redacted] at First Caribbean International Bank, St. John's, Antigua.

33. Two days later, on February 7, 2019, CW-1 withdrew the following funds from the Sant-0965 Account: (i) $8,500 at a Santander branch in Dedham – Route 1; (ii) $9,000 at a Santander branch in Dedham; (iii) $800 at a Santander branch in Randolph; (iv) $800 at a Santander branch in Randolph; and (v) $300 at a Santander branch in Randolph. Following these withdrawals, there was $26.78 left in the Sant-0964 Account.

34. Bank records indicate that there have been no further deposits or transfers of funds into the Sant-0965 Account, nor any activity consistent with the operation of a legitimate business (for "interior design" or otherwise).

35. As of April 24, 2019, the balance of the Sant-0965 Account was -$147.91.

## IV. The Target Subject Directs CW-1 To Open TD Bank Accounts

36. On or about January 17, 2019, at Minang's direction, CW-1 opened another bank account, at TD Bank, in the name of "BRF Global SA," account number ending in 9777 (the "TD-9777 Account").

37. Bank records indicate that CW-1 provided to TD Bank a copy of the same Business Certificate for "BRF Global SA," dated November 23, 2018, that CW-1 had provided to Santander Bank.

38. TD Bank indicated that the TD-9777 Account was not funded and, as a result, the account was closed on or about March 4, 2019.

39. On or about March 9, 2019, CW-1 texted "Africa" on WhatsApp: "And are we done with Santander??" "Africa" replied: "Not yet hun[.]"[3] CW-1 wrote back: "Anything for Santander? Or we're not using it anymore? … Just Td now?"

40. On or about March 13, 2019, CW-1 texted "Africa" on WhatsApp: "Hey how much did you spend at the hookah bar? … You can take it from my part when TD comes in[.]"

41. On or about March 25, 2019, at approximately 4:35 pm, "Africa" texted CW-1 on WhatsApp: "Please send me the TD login and password[.]" Approximately 18 minutes later, "Africa" texted CW-1: "Do you have the login saved on your browser? … Try logging in from your phone and send me a screenshot[.]" Approximately 23 minutes after that, "Africa" texted CW-1: "Still on phone with them?"

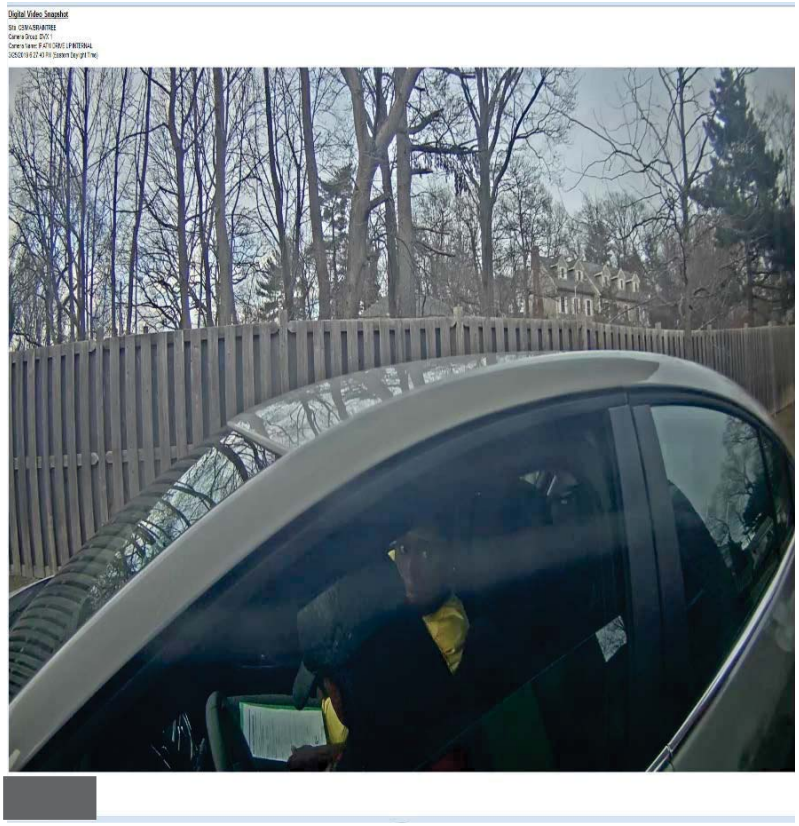
42. At approximately 5:45 pm, CW-1 texted "Africa" on WhatsApp: "They have to set up a new one … He said it will be quick … They have all the info[.]" "Africa" replied: "Ok then[.]"

43. Bank records show that on that same day, CW-1 opened a second TD Bank account, also in the name "BRF Global SA," account number ending in 3199 (the "TD-3199 Account").

[3] All apparent typos and other errors in the text messages quoted herein are reproduced as in the original.

44. Bank records also show that on March 25, 2019, at approximately 6:29 pm, a cash deposit was made to the TD-3199 Account in the amount of $65, at a drive-through ATM at the 405 Franklin Street, Braintree, Massachusetts, TD Bank branch.

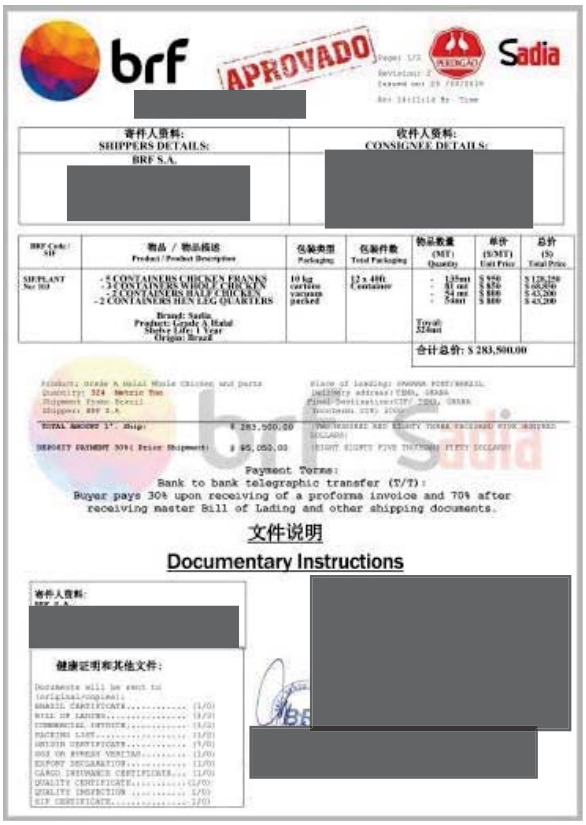
45. The following are surveillance photos of the drive-through ATM area from March 25, 2019 at approximately 6:30 pm, which CW-1 reviewed with the FBI. CW-1 identified the individual in the driver seat as CW-1, and the individual in the passenger seat as Minang:




V. [redacted] Wires Funds To The TD-3199 Account Based On A Fraudulent Invoice

46. Meanwhile, on or about March 25, 2019, [redacted], a company based in Houston, Texas, received an invoice from an email address with the domain name "brf-globalfoods.com".

47. The invoice, in the amount of $283,500, was purportedly for chicken products. It directed that a deposit, in the amount of $85,050, be sent to the TD-9777 Account, which was listed with address in Mount Laurel, New Jersey. The following are images of the front and back of the invoice:





48. A [redacted] employee has advised the FBI that he understood the invoice to be for the purchase of 12 containers of meat product from Sadia, a food company owned by the real BRF Global SA. The [redacted] employee indicated that the meat product was to be shipped from Brazil to the [redacted] facility in Ghana, and was supposed to arrive on or about May 5, 2019.

49. According to records from open source databases reviewed by the FBI, BRF Global's actual domain name is "brf-global.com," which has been registered to the company since July 2014. By contrast, the brf-globalfoods.com domain name from which the March 25 email was sent was registered on or about October 31, 2018 to Domains By Proxy LLC, a third-party domain name registrant. As noted on its website, Domains By Proxy permits domain registrants to register domain names while keeping their identities private. Based on my training and experience, I am aware that third-party domain name registrants are often used by individuals or entities seeking to shield their identities, including for purposes of fraud.

50. Later on March 25, 2019, [redacted] received another email from an address with the brf-globalfoods.com domain name stating: "We will like to inform you that due to financial reviews, BRF S.A incoming payment account is under auditing and during this period, the finance department will like to redirect payment to the account details stated on the revised proforma invoice." The second e-mail directed [redacted] to remit its payment *not* to the TD-9777 Account, but instead to the TD-3199 Account.

51. One day later, on or about March 26, 2019, the TD-3199 Account received an incoming wire in the amount of $85,050 from [redacted] reflecting the deposit that company placed on the meat products it sought to purchase. The wire beneficiary was identified as BRF Global SA in Brazil.

52. On or about March 27, 2019, CW-1 texted "Africa" on WhatsApp, "It's here," with a photo of an ATM screen showing the balance in the TD-3199 Account.

53. On or about March 28, 2019, "Africa" texted CW-1 on WhatsApp: "Talked with connect and he recommended we don't do anything tomorrow" and "We can start cashing out on Friday[.]"

54. On or about March 29, 2019 (a Friday), "Africa" and CW-1 had the following text exchange on WhatsApp:

CW-1: What are we doing today again???

AFRICA: BANK NAME: MILLENNIUM BCP
NAME: [redacted]
IBAN: [Ending in] 89 05
BIC/SWIFT: BCOMPTPL
COUNTRY: PORTUGAL
ADDRESS: [redacted] 8135-104 Almancil

AFRICA: I'm next to the phone if you need any info

CW-1: Ok

55. Later that same day, CW-1 texted "Africa" on WhatsApp that CW-1 was at the bank, and then wrote: "I need the address for the person[.]" At approximately 2:56 pm, "Africa" replied, "Ok hold.on," and then approximately three minutes later, he wrote to CW-1: "[redacted] 156-104 Algave Portugal[.]"

56. On or about that same day, $15,000 in cash was withdrawn from the TD-3199 Account at a TD Bank branch in Norwood, Massachusetts. Bank surveillance footage shows CW-1 in the Norwood TD Bank branch at around the time of the withdrawal and leaving the branch with cash in hand.

57. CW-1 reported that every time CW-1 withdrew cash from the bank accounts, CW-1 provided the funds to Minang, who, on occasion, returned a percentage of those funds to CW-1.

58. The following day, March 30, 2019, CW-1 texted "Africa" on WhatsApp that CW-1 was going to "go to the branches in Quincy and Weymouth," and wrote, "$12,000 and $9,000 right?" "Africa" replied, "Yes perfect," adding: "Today is Saturday so some branches may be like 'it's a weekend and we don't have enough cash etc' – if any branch says that just get whatever max they can give you[.]"

59. That same day, $21,000 in cash was withdrawn from the TD-3199 Account at a TD Bank branch in Quincy, Massachusetts. Bank surveillance footage shows CW-1 in the Quincy branch that day and leaving the branch with cash in hand.

60. On or about April 1, 2019, at approximately 8:17 a.m., bank records indicate that $34,453.06 was transferred via wire from the TD-3199 Account to [redacted], at Millennium Bcp Bank in Portugal, per the instructions provided by "Africa" in the text message above.

61. That same day, there were two cash withdrawals from the TD-3199 Account: (i) $8,200, at a TD Bank branch in Braintree, Massachusetts, at approximately 3:50 p.m.; and (ii) $500, from the drive-through ATM at the TD Bank branch in Quincy, Massachusetts, at approximately 4:13 p.m.

62. On or about April 3, 2019, "Africa" and CW-1 had the following text exchange on WhatsApp:

AFRICA: We should get confirmation for 200 today

CW-1: Ok hun

AFRICA: 198 confirmed

AFRICA: Should be in tomorrow

63. On April 3, 2019, the TD-3199 Account received a second wire from [redacted], in the amount of $198,450. The wire again identified the intended beneficiary as BRF Global SA in Brazil.

64. On or about April 4, 2019, "Africa" texted CW-1 on WhatsApp: "Please check balance at atm when you get up[.]" Approximately four hours later, CW-1 texted "Africa" a photo of an ATM screen showing a "Current Balance" of $198,506.56 and "Available Balance" of $198,320.46.

65. "Africa" responded, "Nice," and then added: "Connect wants us to do 1 wire before you leave tomorrow … Then we can continue the process when you return[.]"

66. On or about April 5, 2019, two wires were sent from the TD-3199 Account to individuals in Barcelona, Spain: one, in the amount of $62,620, to [redacted], and the other, in the amount of $57,350, to [redacted].

VI. TD Bank Asks Questions And Is Given A Fraudulent Invoice

67. On or about April 8, 2019, CW-1 was contacted by a representative of TD Bank concerning the TD-3199 Account. That same day, CW-1 texted "Africa" on WhatsApp that "The lady at the bank said she's calling to confirm the wire[.]" The following text exchange ensued:

AFRICA: Have the info handy

AFRICA: Sender etc

AFRICA: That's crazy

CW-1: Which info

AFRICA: Sender

CW-1: I don't have that

AFRICA: [redacted]

CW-1: ???

AFRICA: TEXAS

CW-1: Ok cool

68. CW-1 then texted "Africa" that the bank was calling "to verify," and "Africa" responded that he "just spoke with [his] friend," and that "[h]e tried calling the client but client was busy[.]" "Africa" added: "He said should not be a problem because when [they] call the client he will confirm everything and it will be released[.]"

69. The following day, April 9, 2019, CW-1 spoke again with a representative of TD Bank concerning the TD-3199 Account. At approximately 11:38 a.m., CW-1 and "Africa" had the following text exchange on WhatsApp:

CW-1: Can you send me an invoice for the wire

CW-1: The lady is asking for it

AFRICA: Wtf

CW-1: She said the lady is about to ask me questions

AFRICA: Why you talking to her?

AFRICA: I told you hold om

AFRICA: I domt have the info

AFRICA: They still preparing everything

AFRICA: You not supposed to talk to them now

CW-1: I told them to hold on

CW-1: So send it

AFRICA: Nah y ok u didn't have to take the call smh

CW-1: Relax I told them to hold on

AFRICA: If you cant calm down and be patient we will lose everything

AFRICA: Trust me

CW-1: They just need an invoice

AFRICA: And we don't need to give them one

AFRICA: That's the problem

AFRICA: I said not to talk to them

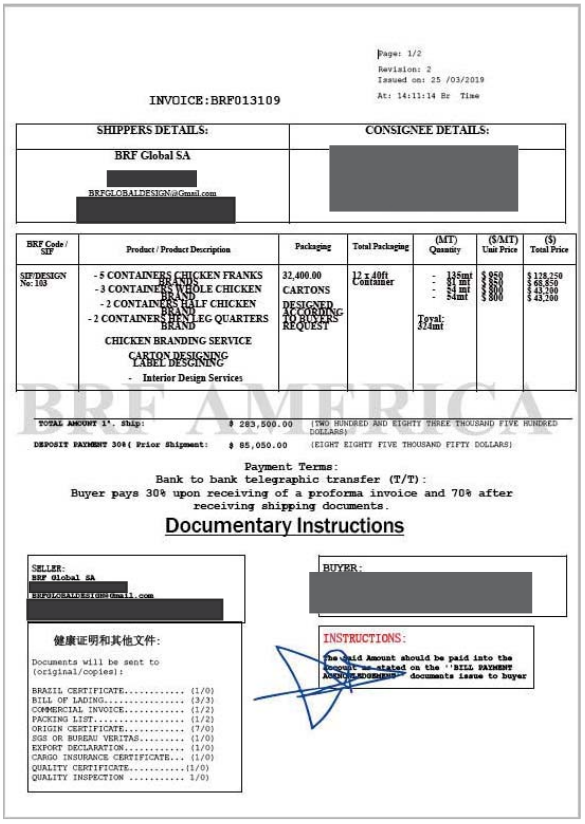
70. At Minang's direction, CW-1 created the email address, brfglobaldesign@gmail.com, for the purpose of communicating with representatives of TD Bank.

71. That afternoon, at approximately 1:39 p.m., "Africa" texted CW-1 on WhatsApp, "What's the address on the account ?" CW-1 replied: "BRFGLOBALDESIGN@Gmail.com,"

adding: "Just created the gmail account[.]" CW-1 then texted, "You can send it to the gmail," and "Africa" replied, "Ok[.]"

72. Just 38 minutes later, at approximately 2:17 pm, the newly-created email address, brfglobaldesign@gmail.com, received an email from financedept@brf-sadia.com, which attached a copy of a purported invoice to [redacted]. The invoice included CW-1's name and address, as well as the brfglobaldesign@gmail.com email address. The invoice listed 12 containers of chicken products, chicken branding service, carton designing/label designing, and interior design services.

73. The following is an image of the front and back of that invoice:



Page: 1/2
Revision: 2
Issued on: 25 /03/2019
At: 14:11:14 Hr Time

INVOICE:BRF013109

| SHIPPERS DETAILS: | CONSIGNEE DETAILS: |
|---|---|
| BRF Global SA | [redacted] |

| BRF Code / SIF | Product / Product Description | Packaging | Total Packaging | (MT) Quantity | ($/MT) Unit Price | ($) Total Price |
|---|---|---|---|---|---|---|
| SIF/DESIGN No: 103 | - 5 CONTAINERS CHICKEN FRANKS BRAND<br>- 3 CONTAINERS WHOLE CHICKEN BRAND<br>- 2 CONTAINERS HALF CHICKEN BRAND<br>- 2 CONTAINERS DRUMLEG QUARTERS BRAND<br>CHICKEN BRANDING SERVICE<br>CARTON DESIGNING<br>LABEL DESIGNING<br>- Interior Design Services | 32,400.00 CARTONS DESIGNED ACCORDING TO BUYERS REQUEST | 12 x 40ft Container | - 135mt<br>- 81 mt<br>- 54 mt<br>- 54mt<br>Toyal: 324mt | $ 950<br>$ 850<br>$ 800<br>$ 800 | $ 128,250<br>$ 68,850<br>$ 43,200<br>$ 43,200 |

TOTAL AMOUNT 1'. Ship: $ 283,500.00 (TWO HUNDRED AND EIGHTY THREE THOUSAND FIVE HUNDRED DOLLARS)
DEPOSIT PAYMENT 30%( Prior Shipment: $ 85,050.00 (EIGHT EIGHTY FIVE THOUSAND FIFTY DOLLARS)

Payment Terms:
Bank to bank telegraphic transfer (T/T):
Buyer pays 30% upon receiving of a proforma invoice and 70% after receiving shipping documents.

Documentary Instructions

SELLER:
BRF Global SA
[redacted]

BUYER:
[redacted]

健康证明和其他文件:

Documents will be sent to (original/copies):

BRAZIL CERTIFICATE..... (1/0)
BILL OF LADING..... (3/3)
COMMERCIAL INVOICE..... (1/2)
PACKING LIST..... (1/2)
ORIGIN CERTIFICATE..... (7/0)
SGS OR BUREAU VERITAS..... (1/0)
EXPORT DECLARATION..... (1/0)
CARGO INSURANCE CERTIFICATE... (1/0)
QUALITY CERTIFICATE.....(1/0)
QUALITY INSPECTION ..... 1/0)

INSTRUCTIONS:
The said Amount should be paid into the account as stated on the "BILL PAYMENT ACKNOWLEDGEMENT" documents issue to buyer

BRF AMERICA

BILL OF PAYMENT ACKNOWLEDGEMENT

This payment of Bill ("The "Acknowledgement") is made and entered into, effective on the date set forth above, by [redacted] (herein referred to as the "Seller") to [redacted] (collectively herein referred to as the "Buyer") Shipping documents to be provided in order to clear the goods at destination port.

BRAND NAME: SADIA

In consideration of the Bill payment of the respective invoice No. BRF013109, the buyer agrees to pay the seller 30% T/T (US $ 85,050.00) "Only" Advance Commitment Deposit at Invoice. We [redacted] acknowledge that the bill payment shall be payable to our Office in USA in charge of all international shipment with Details Account Information as Below:

REVISED ACCOUNT INFORMATION FOR PAYMENT:

| | |
|---|---|
| BANK NAME | *TD BANK* |
| ACCOUNT NAME: | BRF GLOBAL SA |
| ACCOUNT NUMBER: | [redacted]3199 |
| ROUTING NUMBER: | 031101266 |
| SWIFT CODE: | NRTHUS33XXX |
| BANK ADDRESS: | 6000 ATRIUM WAY MOUNT LAUREL, NJ 08054, USA |

AMOUNT 30%: $ 85,050.00

BALANCE 70%: $ 198,450.00

TITLES AND SUBTITLES. The titles and subtitles used in this letter are used for convenience only and are not to be considered in construing.

ENTIRE AGREEMENT; AMENDMENTS: This Acknowledgement (a) constitutes the entire agreement among the parties and no party shall be liable or bound to any other party in any manner by any warranties, representations or covenants except as specifically set forth herein or therein, and (b) may not be modified or amended, except by a written instrument executed after the effective date hereof by the party sought to be charged by such modification or amendment.

SELLER

BRF Global SA
[redacted]

BRF AMERICA

74. CW-1 promptly forwarded this invoice from brfglobaldesign@gmail.com to a representative of TD Bank.

75. On or about April 10, 2019, CW-1 sent an email to TD Bank, stating: "Good morning Samantha, did you receive the requested invoice that was faxed to the number you provided? This has been an inconvenience to our business and causing a loss of revenue." The content of this email, as well as other emails to TD Bank, was directed by Minang.

76. On or about April 12, 2019, "Africa" and CW-1 had the follow text message exchange on WhatsApp:

AFRICA: Let's give them till the end of the day

CW-1: [Unintelligible symbols]

AFRICA: Last time I had a situation like this it took a whole week lol

CW-1: Dam

AFRICA: That's why I'm this patient

77. Between April 10, 2019 and April 24, 2019, CW-1 sent TD Bank additional emails from brfglobaldesign@gmail.com inquiring about the TD-3199 Account.

78. According to a TD Bank employee who spoke with CW-1, CW-1 provided multiple explanations for the [redacted] wires. In one conversation, CW-1 stated that CW-1 designed boxes for [redacted]. On another occasion, CW-1 stated that CW-1 was helping [redacted] with an interior design project. CW-1 also suggested that the bank direct further questions to CW-1's father, who CW-1 said resides in Liberia and owns gas stations in that country. CW-1 said that CW-1's father was CW-1's primary source of business referrals.

79. On or about April 22, 2019, "Africa" and CW-1 had the follow text message exchange on WhatsApp:

CW-1: Nothing yet [sad-face emoji]

AFRICA: Smh damn

AFRICA: I think you should hit Melvin[4] this afternoon if anything to see what's up

CW-1: I already emailed him

CW-1: He said he hasn't heard anything from the lady doing the investigation

AFRICA: Damn

CW-1: The big drop you mentioned went to someone else?

CW-1: [sad-face emoji]

AFRICA: Connect didn't mention

CW-1: [sad-face emoji]

AFRICA: I know

VII. TD Bank Contacts The FBI

80. On or about April 22, 2019 the FBI's Boston Field Office was contacted by TD Bank investigators about a potential BEC fraud involving the TD-9777 and TD-3199 Accounts.

81. As part of its investigation, the FBI contacted [redacted] and spoke with the employee identified as the "company representative" on the invoice received by TD Bank. This [redacted] employee advised the FBI that he did not hire anyone for interior design services, nor did he pay for any branding services (as indicated on the invoice provided to TD Bank).

82. On May 9, 2019, this [redacted] employee advised the FBI that the company had not received any of the product it had purchased.

83. This [redacted] employee also advised the FBI that [redacted] had received an email that purported to be from Golam Shipping, a purported international shipping and logistics

[4] This is apparently a reference to a TD Bank employee whose name appears on the account opening documents for the TD-3199 Account.

company, from an address with the domain name "golamshipping.com." This email advised that the goods reflected on the invoice were being processed by customs in Ghana.

84. According to records from open source databases reviewed by the FBI, the golamshipping.com domain name was registered to WHOIS Privacy Protection Service, Inc., a third-party domain name registrant, on or about February 13, 2019. Like Domains By Proxy, WHOIS Privacy Protection Service permits domain registrants to register domain names while keeping their identities private.

## VIII. The FBI Executes A Search Warrant On CW-1; Minang Then Deletes CW-1's Phone And Tells CW-1 Not To Talk

85. As noted above, on May 20, 2019, FBI agents executed a search warrant on CW-1's person and mobile telephone as CW-1 entered the TD Bank branch at 405 Franklin Street, Braintree, Massachusetts. From CW-1's mobile telephone, the FBI recovered text messages between CW-1 and "Africa," including those described above, as well as other evidence.

86. Following the search, CW-1 contacted Minang to tell him what had happened. That same night, Minang drove to CW-1's apartment, and the two met and spoke in Minang's car outside CW-1's residence.

87. During that conversation, Minang took CW-1's mobile telephone, deleted it, and gave the phone back to CW-1.

88. Minang told CW-1 that CW-1 should not speak with law enforcement, telling CW-1 that it would be bad for CW-1, and bad for him, if CW-1 were to speak. Minang then told CW-1 that CW-1 should get a lawyer, and that they should go their separate ways.

89. CW-1 retained counsel, and then decided to speak with the FBI. CW-1 told the FBI about CW-1's interaction with Minang on the night of the search, and shared additional information concerning the scheme. CW-1 advised the FBI that CW-1 was recruited by Minang

to open the bank accounts described above, and moved money through those accounts at Minang's direction. CW-1 admitted that "BRF Global SA" was not a real business, and that CW-1 created it at Minang's direction for the purpose of opening the bank accounts.

90. On June 19, 2019, in response to a subpoena, Google indicated that the following email addresses were "alternate e-mails" for financedept@brf-sadia.com (the email account from which CW-1 received the fraudulent invoice): international@brf-sadia.com; sadia@brf-sadia.com; international.sales@brf-sadia.com; and sales@brf-sadia.com. The subpoena response also identified the email address, kingofhumanarts@gmail.com, as the recovery e-mail for financedept@brf-sadia.com and export@brf-globalfoods.com (an additional email used to communicate with [redacted]).

IX. Probable Cause That The Target Subject Committed The Target Offense

91. Based on the foregoing facts, I believe that probable cause exists to conclude that Minang, the Target Subject, has conspired with others known and unknown to the government to transport, transmit, and transfer, and attempt to transport, transmit, and transfer a monetary instrument and funds from a place in the United States to and through a place outside the United States, knowing that the monetary instrument and funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission, and transfer was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(h). This is based on the facts set forth above showing Minang's role in directing the transfer of funds to and from the Sant-0965 and TD-3199 Accounts to and from accounts outside the United States, knowing that the funds involved were the proceeds of fraudulent activity, *i.e.*, a BEC scheme.

***THE PREMISES CONTAINS EVIDENCE, FRUITS, AND INSTRUMENTALITIES***

92. I also have probable cause to believe that the premises to be searched contains fruits, evidence, and instrumentalities of violations of the federal statutes listed above, as described in Attachment B.

93. As part of the conditions for his release, Minang is required to be at his residence between 4 a.m. and 6 am. He has been fitted with a monitoring bracelet to confirm his compliance with this condition. Because Minang will be at his residence at 6 a.m., there is probable cause that he will have one or more mobile phones with him at his residence at that time, including mobile phones that he used in furtherance of one or more BEC schemes.

94. Based on my training, experience, and information provided by other law enforcement officers, I know that participants in BEC schemes often retain records relating to such schemes in their residences. Here, I believe that the Target Subject's residence likely contains bank records and other documentation relating to BEC schemes, including documentation relating to the Santander and TD Bank accounts described above. I further believe that the Target Subject's residence likely contains records pertaining to the existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the Target Offenses. In addition, I further believe the Target Subject's residence may include fruits of the Target Offenses, including cash and evidence of extravagant purchases by the Target Subject.

***SEIZURE OF COMPUTER EQUIPMENT AND DATA***

95. Based on my training, experience, and information provided to me by other law enforcement officers, I know that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and

updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online. I am also aware of statistics published by the U.S. Census Bureau estimating that as of 2015, approximately 87 percent of households had a computer (desktop, laptop, handheld, or other).

96. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones, and storage media.

97. Based on my training, experience, and information provided by other law enforcement officers, I know that many smart phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers.[5] Smart phones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, and web browser; sending and receiving text messages, e-mails, and other communications via specialized communication apps; and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

98. As described above, the Target Subject has used at least one smart phone in furtherance of the Target Offenses. Moreover, the Target Subject has used multiple phone numbers and mobile phones, which may be present in his residence and contain evidence relevant to the Target Offenses.

[5] References to "computers," "computer equipment," and "computer hardware" herein are intended to include smart phones.

99. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the internet. This is true because:

a. Electronic files that have been downloaded to a storage medium (including the memory of a smart phone) can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the internet are sometimes automatically downloaded into a temporary internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed internet pages or if a user takes steps to delete them.

100. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence—storage media including memory cards and the internal memory of smart phones—can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements—analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring

expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap." Smart phones can easily be remotely "wiped" removing all data and essentially returning a device to its original factory settings. Consequently, law enforcement agents may seize the computer equipment for subsequent processing elsewhere.

101. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

## CONCLUSION

102. Based on the information described above, I have probable cause to believe that that the Target Subject has engaged in and continues to engage in the Target Offense.

103. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of the Target Offenses, described in more detail in Attachment B, are located at the residence of the Target Subject, described in Attachment A.

I declare that the foregoing is true and correct.

Andrea Sciolino
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 28th day of June, 2019

HON. DONALD L. CABELL
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**DESCRIPTION OF THE PREMISES TO BE SEARCHED**

The premises to be searched are located at 319 Lincoln Street, Apartment 231, Hingham, Massachusetts. The building at 319 Lincoln Street, Hingham, Massachusetts is a five-level residential apartment complex. Apartment 231 is a 1,097 square-foot, 2 bedroom, 2 bathroom unit on the second level of the complex.

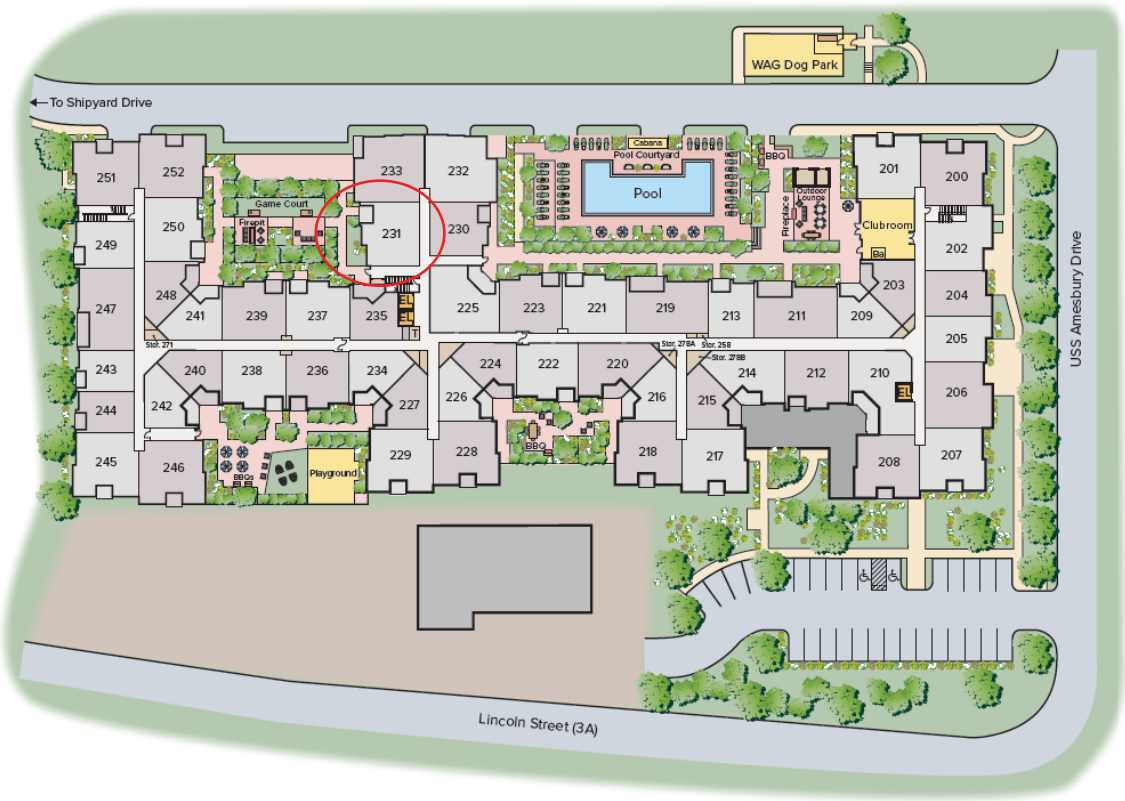
The following are two photographs of the primary entrance to the apartment complex, on Lincoln Street:


The following is a floorplan for the second floor of the apartment complex, showing where Apartment 231 is located:

AVALON

RESIDENCES AT THE HINGHAM SHIPYARD

2ND FLOOR




We would like to take you on a standard tour route that may include a model apartment and many community amenities. If you wish to alter this route, see a specific apartment or see other community features, we can do so upon request.

This plan is intended for illustrative purposes only.

319 LINCOLN STREET • HINGHAM, MA 02043 • 781-739-3540

The following is a floor plan of Apartment 231:

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 1343 (Wire Fraud), 1349 (Wire Fraud Conspiracy), 1956 (Money Laundering), 1956(h) (Money Laundering Conspiracy), and 1512 (Witness Tampering) (collectively, the "Target Offenses"), including:

A. Records and tangible objects pertaining to the following people, entities, telephone numbers, bank accounts, domain names, and email addresses:

1. Santander Bank (including but not limited to account number ending in 0965, and any accounts in the name of BRF Global);
2. TD Bank (including but not limited to account numbers ending in 9777 or 3199, and any accounts in the name of BRF Global);
3. BRF Global;
4. BRF SA;
5. Sadia;
6. Cvale SA;
7. [redacted];
8. [redacted];
9. [redacted];
10. [redacted];
11. [redacted];
12. [redacted];
13. [redacted];

14. [redacted]

15. [redacted]

16. [redacted]

17. [redacted];

18. Businesses registration records;

19. brfglobaldesign@gmail.com; export@brf-globalfoods.com; financedept@brf-sadia.com;

20. international@brf-sadia.com; sadia@brf-sadia.com; international.sales@brf-sadia.com; sales@brf-sadia.com; kingofhumanarts@gmail.com;

21. brf-sadia.com; brf-globalfoods.com; brf-global.com; and golamshipping.com;

22. [redacted];

23. [redacted]; and

24. [redacted].

B. Records and tangible objects pertaining to the payment, receipt, transfer, or storage of money or other things of value by the Target Subject or any co-conspirators, including:

1. Bank, credit union, investment, money transfer, and other financial accounts;

2. Credit and debit card accounts;

3. Money remittances through money service businesses (e.g., Western Union or MoneyGram);

4. Tax statements and returns;

5. Business or personal expenses;

6. Income, whether from wages or investments;

7. Loans;

C. Records and tangible objects pertaining to the existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the Target Offenses;

D. Records showing the relationship between the Target Subject and any co-conspirators, including records of their travel and meetings, calendars, address lists, contact lists, photographs, social media contacts, and identities and personal identifiers used by each (including telephone numbers, usernames, and social media profile information);

E. Records of communications between the Target Subject and any co-conspirators in furtherance of the conspiracy;

F. All negotiable instruments, including United States currency, if found in aggregate of $5,000 or more;

G. For any computer hardware, computer software, mobile phones, smart phones or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the

presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of when the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

7. records and tangible objects pertaining to accounts held with companies providing internet access or remote storage; and

II. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

## DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, mobile phone, smart phone, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smart phone, mobile phone, or wireless communication device); any peripheral input/output device (such as a drive intended for removable storage media); and any security device, (such as electronic data security hardware).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

## RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.